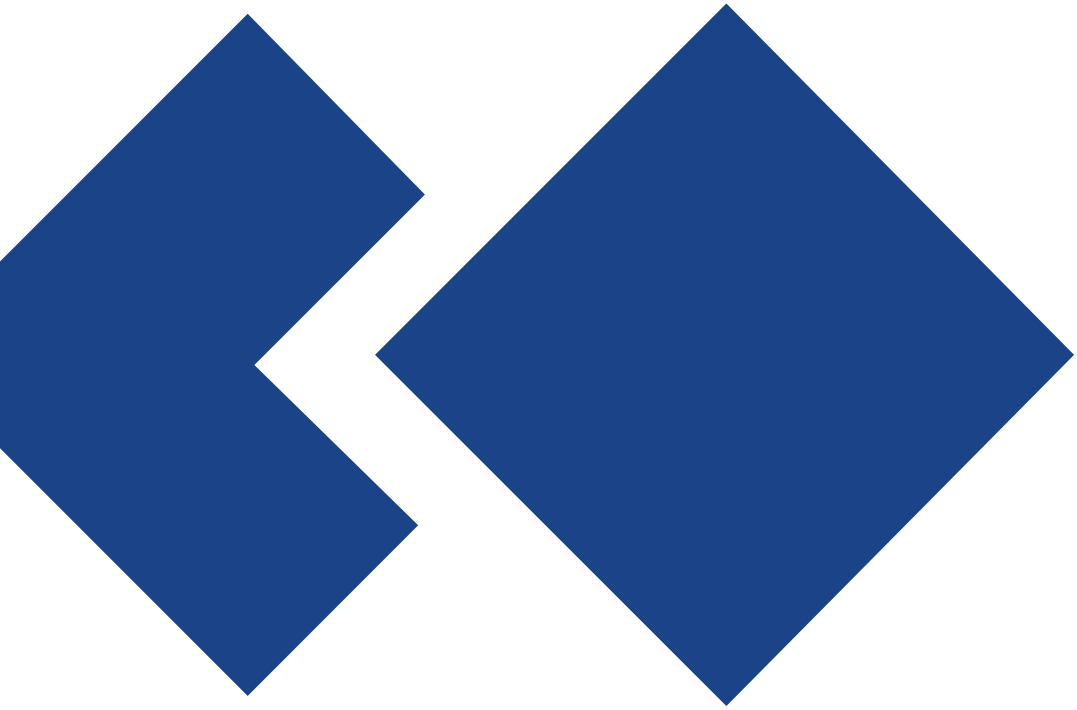
Steps to Improve D/3® DCS Cyber Security

White Paper



NovaTech®

Experts in Batch Process Automation, Flexible Recipe Driven Continuous Automation, Procedural Automation, Substation Automation, and Electrical Instrumentation.

Serving the Agriculture, Biofuels, Brewing, Chemical, Energy, Metals, Pharmaceutical, Power Distribution, Nuclear and Steel Industries.

NovaTech

novatechweb.com

TABLE OF CONTENTS

INTRODUCTION

It is fair to say that without a fully functional distributed control system (DCS), a modern plant cannot operate safely and efficiently and, in some cases, cannot operate at all. Therefore, it is vital to ensure the integrity of all DCSs and protect them from malicious attacks, accidental corruption, and data breaches that may jeopardize safety or production or may compromise the end user's competitive advantage in the marketplace.

This paper describes the philosophy and guidelines for keeping your D/3® DCS secure from cyberattacks.

DCSs have come a long way from the days of panel boards and pneumatic instrumentation. Most customers work with the latest computer technology on a daily basis through their personal electronic devices and expect similar features and capabilities from their DCSs.

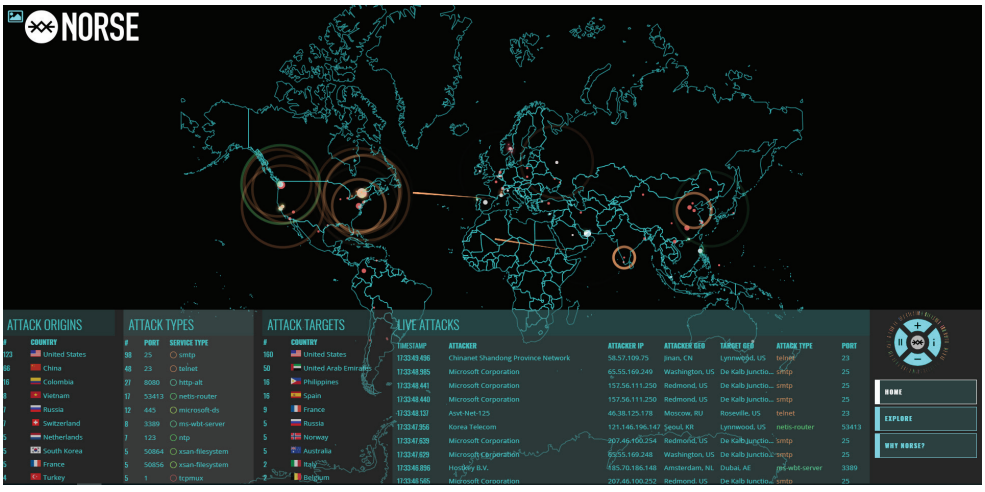
Modern DCSs are like the central nervous system of a plant. They provide for plant and personnel safety using sophisticated safety systems, interlocks, and alarm systems. They provide for efficient plant operation through high performance Human Machine Interfaces, recipe and batch management, and equipment control. Furthermore, a typical DCS stores vast amounts of proprietary information such as product recipes, process steps, graphics, historical data, alarm history, design documents, and help documentation, etc.

RISK ANALYSIS

Although most end users consider their DCSs secure, vulnerabilities exploited in commercial system attacks serve as a warning for all computer system managers. Each control system should be evaluated for possible risks from external and internal sources and measures introduced to counteract those risks as part of a comprehensive Cyber Security risk management program. Whether accidental or intentional, human interaction by operators, managers, engineers, technicians, IT staff members, contractors, and other outside parties has the potential to cause significant damage to DCS operation and data integrity.

To help implement best practices in network design, access control, and countermeasures, review Cyber Security industry standards such as NIST SP 800-82.

To see real-time, global cyber attacks at industrial sites, visit www.norsecorp.com



To identify potential vulnerabilities, perform a DCS Cyber Security risk analysis, similar to a Process Safety Management (PSM) analysis. This study should list all possible threats, quantify their impact and identify risk mitigation actions for each threat. This risk analysis should be conducted and updated periodically. Risk analysis tools such as the ICS-CERT Cyber Security Evaluation Tool can help with performing a comprehensive DCS risk analysis. A sample Security Maintenance Checklist included later in this document provides suggestions for the scope of the analysis.

PHYSICAL SECURITY

The most obvious method of protecting DCS resources is to physically secure the equipment. The plant may already have a method of limiting physical access, but once someone is in the plant, can they access data, computers, network gear, controllers, or I/O? Each physical component of the DCS should be in a locked cabinet or placed in a limited access area and provided back-up power. This includes, but is not limited to, all DCS network components, process controllers, servers, and operator consoles. New generations of I/O communicate directly through gateways to the DCS. Users should perform an audit to ensure that these gateways are physically secured as well. In addition to limiting physical access to DCS equipment, disabling/limiting ports and removing/disabling CD/DVD devices and any other means for introducing external software directly into the DCS should be completed.

The DCS system administrator and his/her backup should keep a list of all personnel with key access to these areas and cabinets to control and manage key distribution. Periodic checks of the DCS physical security should be part of an overall Cyber Security/DCS maintenance program.

NETWORK DESIGN AND SYSTEM CONFIGURATION

Given that physical access to the equipment is properly restricted, it is still possible to access the DCS externally. The network that connects all the components of the control system and connects the DCS to external systems is a vulnerability that should be analyzed.

The most obvious way to prevent external threats to the control system through the network is to ensure the entire DCS System is air-gapped. Although this is done in some very secure environments, it is not practical in many of today's modern plants where external access to DCS data is required. In these cases, implementation of a network buffer zone (commonly referred to as a demilitarized zone or DMZ) with firewalls between the control system and any other systems will help reduce the risk of an external threat while providing inter-system communication. For example, NovaTech provides an integrated OSIsoft-PI interface. This feature allows the PI server to be installed in the DMZ and act as an intermediary between the DCS and business systems requiring access to control system data.

Firewalls should be implemented in all layers of a plant including the DCS network and DCS computers. Firewall appliances, such as those from Tofino, can be installed between the servers, controllers and I/O sub systems to help eliminate or at least limit intrusions from unknown computers or programs. These industrial firewalls are designed to perform both protocol and deep packet inspection to control and limit communications to and from the various DCS components. Starting with D/3 Version 16 (D3v16), the D/3's PCM5 uses an automatically configured Linux-based IPTables firewall. This basically prevents any non-D/3 node from communicating with or remotely logging into the Process Control Module. Existing D/3 users should plan to upgrade to newer versions of D/3 which include these built-in firewalls at the process controller level.

The network addresses assigned to the nodes of a DCS should be non-routable static addresses. Dynamic Host Configuration Protocol (DHCP) on a DCS is highly discouraged as it could provide an avenue into the DCS network. Additionally, by assigning only static IP addresses, each computer's network activity can be monitored and tracked. Users may also consider reassigning all standard ports used by common applications, such as 8081 and 1433, and configure other ports to communicate with these applications.

Windows security has improved with each new operating system. D3v16 runs on the Microsoft Windows Server 2016 platform which provides D/3 with the most recent generation of Windows security through enhanced group policies and built in Windows firewall protection. Proper system configuration will ensure security features are protecting the DCS.

A DCS security plan should include an antivirus application that can protect against malware without negatively impacting the memory or performance of the computer. NovaTech currently uses Microsoft's Defender. Customers using the D/3 have also used Symantec Endpoint and McAfee antivirus software. An alternative to the traditional, reactive blacklisting antivirus is the use of proactive whitelisting approach such as Carbon Black applications whitelisting. This application allows the user to list all applications allowed to run on a computer (whitelist). Any other application that is introduced, whether malicious (zero-day attack) or not, will not run on the computer and the software produces alarms and records the execution attempt in a log for later review. Information on the D/3 executable programs and services that must be included in exclusion list for the D/3 software to function properly is included in the installation documentation.

Of course, anti-virus and anti-spyware operations add additional load to the computer. The system should be checked to ensure that any software added to a D/3 system does not diminish the real time operation of the D/3. Benchmark testing of the D/3 software is recommended before and after any additional software is installed, such as PI, anti-virus or anti-spyware packages to determine that time critical D/3 functions are not affected.

IDENTITY AND ACCESS MANAGEMENT

It is very important to manage and maintain individual user accounts for anyone accessing or using the DCS. All unused standard user accounts such as Administrator, Guest, D3Administrator, D3Operator, and D3Maint should be disabled and all generic passwords removed. Keep a record of DCS system
administrator user credentials in a safe and secure location to allow access to a system administrator privileged account in the event of personnel changes. Since each D/3 user can be associated with user groups (whether in a domain or a workgroup). D/3 users should be added to the appropriate group based on their role in the organization. Note that a different set of privileges can be assigned to each user or user group. Example user groups are as follows:

1. System Administrators
2. D/3 Administrators
3. D/3 Engineers
4. D/3 Operators
5. Boiler Room Operators
6. Line 1 Operators
7. Instrument Technicians
8. Supervisors

After assigning each user an individual login account, everything that the user does on the D/3 System is logged under the respective username and all actions are time stamped accordingly. Log files are easily searched for all activities performed by a certain user. The D/3 DCS features extensive logging of all operator and most engineering activities. The D/3 allows operator console protection to be configured by groups. This is a very convenient way to set up privileges for certain classes of users and then assign each individual user to those groups. Note that users can belong to multiple groups.

Once policy settings are defined, ensure proper control and management of user access credentials and privileges. Immediately remove accounts for users who should no longer access the system. Require users to change passwords periodically. Multi-factor user authentication, which requires both something the user knows (password) and something the user has (token), is another security enhancement to consider mitigating compromised passwords. For extra isolation, D/3 DCS user credentials should not be the same as the user's corporate credentials.

CONTROL SYSTEM CONFIGURATION MANAGEMENT

With the DCS equipment physically secured and the external threat addressed, it is time to consider internal threats. In addition to implementing whitelisting, D/3 customers can implement custom user profiles and group policies to limit application execution. Disabling AutoPlay and USB ports and requiring login password complexity and password reset are just some of the policy settings designed to increase security. Limiting access to applications is only one part of mitigating an internal threat. Some users require full access to the system for enhancements, troubleshooting, and repair while others only require access to certain system functions. NovaTech can assist customers with these and other policy settings to ensure secure operations of their D/3 DCS.

Configuration Management is a fundamental tool for ensuring the correct application files are installed and maintained on the production DCS. The D/3 includes the ability to integrate several of the most common source control configuration management tools on the market. Where possible, a separate development control system with a medium fidelity simulation (commonly written in SABL) should be employed. This development system allows users to develop and test code and configuration modifications without jeopardizing the integrity of the actual DCS. The configuration management tool can be used to ensure only specific changes are implemented. Additionally, remote access to a development/testing system via VPN would provide secure access for development and troubleshooting without compromising production system integrity. NovaTech has installed several development/test systems on virtualized platforms to provide a more cost effective, reliable solution.

With respect to operations, customers should consider limiting DCS equipment access and control to certain areas of responsibility. For example, utilities operators should be able to manage and control boiler equipment but not production line equipment. Likewise, production operators should not be able to control utilities area equipment. The D/3 DCS can limit which consoles can control certain equipment thereby restricting access to an operator's respective area of responsibility. By specifying (and possibly even dynamically adjusting) the Console Enable Index of a process unit or specific tag, system engineers can prevent inadvertent operation of equipment outside of an operator's area of responsibility.

RECOVERY PLANNING

Users should consider disaster recovery in the overall Cyber Security plan. The D/3 is designed to distribute functionality across the various nodes of the system and virtually everything can be made redundant. Therefore, no single point of failure should significantly impact plant operations. In the event of a complete disaster such as a fire, hurricane, flood, or severe cyberattack, a comprehensive disaster recovery plan can help the customer resume operations as quickly as possible. A fundamental part of this plan must be a data backup plan. Daily incremental backups as well as weekly full backups should be automatically scheduled and both onsite and offsite storage locations should be established. Users should also consider how all DCS network switch, gateway, PLC, and even field device settings are documented and backed up and include these in the overall data backup plan.

Using a development/training system as a hardware backup location, including replacement servers, operator stations, controllers, switches, and gateways provides the plant with a robust and responsive backup source that is already proven and ready to install. With the backup process in place, it is vital to test the backed-up data on a regular basis and ensure it can be recovered. Backups are useless if the data cannot be retrieved properly and efficiently.

Create and maintain a disaster recovery plan including:

- Designated personnel and action plans
- Backup hardware
- Software backups (onsite, offsite)
- Safe and secure location of system administrator user credentials
- Safe and secure location of physical media
- Separation of physical equipment (servers, operator workstations, network gear)

SECURITY MAINTENANCE CHECKLIST

With the best security measures in place, there is still no substitute for due diligence. Threats will continue to evolve and even the best countermeasures of today will not be the best countermeasures of tomorrow. Regular (weekly) review of Windows application, Windows security, and Windows system logs should be performed. Periodic (twice daily) review of D/3 System alarms should also be performed. Additional logs associated with networking traffic and control system performance should be included in a regular review.

Even if the DCS is isolated, software updates should be done on a regular basis, to address enhancements or patches to existing the Operating System and support software. Regular scanning of the system for any previously unidentified issues is also encouraged. If antivirus software is employed on the DCS, virus definitions must be updated on a regular basis. All major antivirus software managers have a mechanism for updating the definitions offline.

Ensure proper setup and maintenance of your D/3 DCS. Customers should also consider working with NovaTech to create a checklist and action plan to ensure that their D/3 System is configured properly

and stays up to date and in top operational condition. A list of Microsoft updates tested on the D/3 may be found here:
https://support.novatechps.com/Products/dcs/MSUpdates/MSUpdatesTested.htm

A boilerplate checklist for consideration follows:

D/3 System
- Review configuration (ensure Cyber Security and recommended system settings)
- Review system alarms (twice per day)
- Review spare capacity (HW, I/O, CDB, SDB, SABL®) quarterly
- Init/Monitor/Watchdog programs in place and up to date
- Develop plans for next scheduled plant outage
- D/3 patches (required/installed)

Process Controllers (PCMs)
- Physical access
- Network
- Power & power supply analysis
- Memory/CPU usage
- Spare capacity analysis
- Recovery plan for failed PCM

Servers
- Microsoft patches
- Review access logs
- Antivirus/whitelist
- RAID disk status and spare disk space
- Memory analysis
- Physical ports locked down
- Unnecessary applications locked down/eliminated
- User account and credential management
- Backups made
- Daily backup made on CDCM (review integrity)
- Disk cleanup
- Physical inspection of fans, keyboard, mouse, monitor, D/3 keyboard
- Spare parts/spare server
- Recovery plan for failed server

Computers
- MS patches
- D/3 patches
- Antivirus/whitelist
- Disk space/disk cleanup
- Memory
- Physical ports
- Recovery plan for failed computer
- Physical inspection of fans, keyboard, mouse, monitor, D/3 keyboard
- Spare parts/spare computer
- Recovery plan in place

User Account Management
- Review user credential management
- Review user groups
- Review users within groups
- Review user/user group privileges

Network
- Network switch analysis
- Firewall analysis
- Port usage
- Spares (switches, fiber transceivers, fiber, cables, wireless components)
- Documentation/backup of configuration for all network components

Physical
- Rooms
- Cabinets
- Fans in all cabinets
- AC in computer rooms
- Grounding
- Access control list

Disaster Recovery
- Risk analysis
- Disaster recovery plan in place
- Onsite/offsite backup media

Spares Analysis
- Spares in place for all critical system components

CONCLUSION

Today's DCS is a potential target for different entities with varying motivations. Threats range from accidental corruption, deletion or distribution of sensitive data to industrial espionage or even terrorism. While the job of the automation professional has always been demanding, today's world requires added attention to risk management with respect to Cyber Security. Process control engineers should take a proactive approach to Cyber Security, perform a comprehensive risk analysis and develop a plan to minimize and manage Cyber Security threats on their DCSs.

In summary, please consider the following steps to improve D/3 System Cyber Security:
- Evaluate risks – identify risks and remediation to increase Cyber Security
- Ensure physical protection
- Follow good network design and configuration practices
- Manage user access
- Manage control system configuration
- Prepare for disaster recovery
- Be vigilant - create a checklist and perform periodic maintenance and evaluation